KPMG IT Audit Overview and Introduction: A Classroom Exercise

Full Paper

Carey Cole
James Madison University
colecb@jmu.edu

Abstract

This IT auditing case study was created with KPMG and designed for students in an introductory MIS or CIS course. However, it could be utilized for most university students with a general understanding of IT systems. The lecture materials and case study are designed to provide an introduction to the IT auditing process and to challenge teams to examine process documentation and identify relevant IT controls.

Keywords

IT Auditing, IT Auditing Controls, Classroom Case.

Introduction

The StellanTECH Case Study is designed for students in an introductory MIS or CIS course. Many of the Faculty and Student Resources are provided in this paper. Additional resources are available by contacting KPMG.

Module Learning Objectives

This module provides students with an opportunity to:

- Understand what an IT audit is and why IT audits are performed
- Recognize IT systems controls and identify when they are lacking
- Learn about careers in IT auditing

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
<th>Suggested Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lecture</td>
<td>Discussion of IT systems controls and related audit techniques</td>
<td>30 minutes</td>
</tr>
<tr>
<td>Case Study</td>
<td>Students review StellanTECH case study handout</td>
<td>15 minutes</td>
</tr>
<tr>
<td>Exhibit 2</td>
<td>Students review Exhibit 2 – Access Control Documentation and complete the assignment</td>
<td>10 minutes</td>
</tr>
<tr>
<td>Prepare Report</td>
<td>Start to prepare an IT Audit Report using the Template provided. The remainder will be completed as homework.</td>
<td>20 minutes</td>
</tr>
<tr>
<td>Day 1 – Total Time</td>
<td></td>
<td>75 minutes</td>
</tr>
<tr>
<td>Day 2 Discussion</td>
<td>Class discussion on findings and recommendations based on review of the case study</td>
<td>20 minutes</td>
</tr>
</tbody>
</table>

Table 1: Sample agenda: In-class and homework activity

Class structure: 75 minute lecture. This material is flexible in order to meet your needs. The following activities can either be completed during one or two class sessions or primarily online or after class.
Materials Included

Student handouts (included in this submission)
- StellanTECH Case Study – Exhibit 1
- Access Controls Documentation – Exhibit 2
- StellanTECH Critical System Audit Report Template – Exhibit 3

Facilitator Resources (not included in this submission due to space limitations but these are available)
- StellanTECH Case Study – Facilitator Resource
- Access Controls Documentation Exhibit 2 – Facilitator Resource
- StellanTECH Critical System Audit Report – Facilitator Resource – Exhibit 4
- PowerPoint slides
- Leader’s Guide

Format and Presentation of Case Study (Faculty Step-by-Step)

1. Presentation and Classroom Introduction

The instructor may use PowerPoint slides to present an introduction to IT auditing. The presentation includes a discussion of the reasons IT audits are performed and some of the common steps used when conducting an IT audit. The instructor should include a discussion on IT controls in this presentation. The current slide deck includes 22 slides and notes that are available for use. The topics include risks, controls, what is an IT Audit, why are Audits performed, IT Auditor Responsibilities, soft skills and hard skills required to be an IT Auditor. The PowerPoint slides are available upon request from KPMG. The instructor may wish to review Exhibit 4 before beginning the case to review some of the issues and sample replies.

2. Case Introduction

After the concepts for IT Auditing are introduced using the PowerPoint slides, the Instructor may play the first video created for this case (the videos are available upon request from KPMG). In the first video, the founder of StellanTECH greets the IT audit team (your students) and provides company background.

The StellanTECH Case Study (refer to Exhibit 1 below) is then provided to the students to read and review. After the students individually review the case study, the students should form teams (preferably 2-4 students) to further discuss the case. Students are asked to identify security weaknesses within the company’s processes. For each weakness identified, students will document the condition, criteria, and effect of the weakness. The report outline in Exhibit 3 can be given to the students at this time if you wish for them to create a good looking report which is what an Audit team would do.

This case study review can either be done informally as a class discussion or the instructor may choose to assign the student teams to develop a more formal report of their findings. We recommend giving students 10-15 minutes in class to review the case study and think through the control weaknesses.

3. Access Controls Documentation

At this point the students should recognize that they need some more data. You can lead your students to this conclusion. Now it is time to show the second video. In this video, the founder of StellanTECH acknowledges the request from the IT audit team to provide additional support around access controls. The instructor will provide the students with Access Controls Documentation (refer to Exhibit 2 below).

This material is designed to look like sample documentation that has been provided to an IT auditor from their client in an e-mail. Students should review this material to determine whether the controls stated in
the Case Study are operating effectively. Students may work on this assignment in class, if time permits, or complete the assignment as homework.

4. Class Discussion and/or Homework

Either the instructor should collect the case responses and/or have a good class discussion at this time. The instructor should debrief the case study exercise with the class by asking them what security weaknesses they identified and what the effect of those weaknesses could be. In an IT audit, the auditors would design Tests of Controls to determine whether the controls are functioning effectively.

Close the activity by playing the final video vignette. In this video, the client thanks the IT audit team for their recommendations. The purpose of this video is to help students understand the value added by client service professionals.

StellanTECH Case Study – Exhibit 1

Background

StellanTECH (the company) specializes in providing healthcare services and encouraging healthy living by connecting health managers to clients through a proprietary software. The company made waves in the healthcare sector as an IT start-up 6 years ago and has grown significantly. Recently, the company began selling high-end healthcare products as an additional way to support their clientele.

The company is managed by young entrepreneurs and co-founders, Luca Stellan and Blaire Alden. Luca and Blaire met while working at the student newspaper at their alma mater Stanford University. Luca graduated with a Ph.D. in computer science. Blaire studied medicine and completed her M.D/Ph.D. in biomedical informatics. Shortly after graduating, they combined their love of technology and health to launch StellanTECH, named after Luca’s grandfather who encouraged Luca to pursue his dream of earning a Ph.D.

Luca and Blaire started the company on a shoe-string budget. They quickly realized the need for a partner with a business background to help manage the process of raising funds through venture capital investments. They hired Blaire’s childhood friend, Caroline Anderson. Caroline and Blaire grew up together in a suburb of Washington, DC. Caroline obtained her MBA at the Wharton School at the University of Pennsylvania.

As StellanTECH expanded, Luca and Blaire continued to hire friends they knew and trusted. This created a very warm, inclusive corporate culture and makes StellanTECH a great place to work.

The primary computer system at the company is called “Critical”. This system tracks health related and private data for each of their patients. The software is a commercial off-the-shelf application and the data is stored in an Oracle database on a server. The system is hosted in one location within their primary data center within the corporate headquarters in Washington, DC.

The IT Audit

Luca and Blaire heard about your team’s expertise in IT Auditing through their most significant investor. They have requested that you perform an assessment of the IT environment, including relevant controls, to provide process recommendations with a focus on their most important computer system, Critical. This is the company’s first IT controls assessment. Your team has been working together for a very short time, but bring a variety of skills and expertise to the table. This is a terrific client to add to your portfolio.

To get your team started on this project, the IT staff provided you with a summary of relevant controls and processes.
Process Summary

Access Control Process
When hiring a new employee, no background check is performed. The company views everyone as ethical and honest. Prior to gaining access to the Critical system, an end user will request access via their supervisor. Their supervisor will then acknowledge to the administration office for Critical that the end user is an authorized user and that the access that they are requesting is appropriate.

After the initial system access is granted, all further access requests are made directly by the End-User and the administration office for Critical. When an employee no longer works for StellanTECH, their system access is deactivated.

Process Flow

Members of the sales team have end-user access to the Critical system. This enables them to enter data in the Critical system daily to capture the items sold to their specific customers. Sales managers are granted access as power-users and can enter data into the system for all customers. All members of the sales team receive quarterly bonuses based on the number of new customer accounts they create. When a new customer is created, the system automatically scans the other customer names looking for duplicates. If no duplicates are found, the account is marked “new.”

In addition to connecting healthcare managers with their clients, StellanTECH also sells an exclusive line of health supplements. The system tracks the amount and location of each product sold. Every day the inventory is replenished as necessary. There is a separation of duties between various departments. A summary of the products sold and the location are available every day using the corporate data warehouse. Some managers prefer to see their results in a paper report.

Configuration Management Process
Requests for software changes are made in the Rational ticketing tracker which establishes a workflow for change approvers. All changes must be tracked in the Rational ticket tracker. Changes must be approved by the Change Manager (CM) prior to being assigned to a software developer.

After development, changes are reviewed by the Change Control Board (CCB), which meets on a weekly basis, prior to being approved for production. As a note, all software testing is performed in the testing environment and then moved into the development environment. Testing is completed by comparing the software’s functionality to the requirements. The Quality Assurance (QA) team allocates their time testing updates based on which updates are determined to be significant.

After approval, the new version of the software is moved into the Production environment and end-users can use the new software. During the CCB meeting, the change and the testing results are reviewed for the security impact and for the impact on the other systems. Changes must be approved by the CCB prior to implementation into production. This process requires a lot of coordination and takes some time. StellanTECH is in the IT business, so software updates cannot be delayed. The CCB review and approval process is sometimes skipped if the project is running behind.

Contingency Planning Process
Data in the Critical system is replicated every Wednesday from the primary processing site in Washington, DC to an alternate processing site in Omaha, Nebraska on a near real-time basis. The server room is open to all employees to enable easy coverage for the IT team, should someone be out of the office. Critical has a security categorization of High, a recovery time objective (RTO) of 6 hours and a recovery point objective (RPO) of 1 hour. There is a policy that requires that functional tests be performed at least every other year for systems with high security categorizations. Company management has not performed a functional exercise in five years due to resource limitations. The security manager and
program manager performed a test five years ago when they reviewed the contact information in the Information System Contingency Plan.

Instructions:

Identify Conditions/Weaknesses, Possible Effect, and a Recommendation for issue identified.

Note: You may want to provide the students a table similar to the one provided in Exhibit 4 that includes the first line item: When hiring a new employee, no background check is performed.

Access Controls Documentation - Exhibit 2

Your team wants to verify that the StellanTECH system access processes follow their corporate guidelines so you request some data to review via an e-mail. The e-mail thread below includes a sample of 10 people who joined the company within the last month and a sample of 10 people who exited the company in the last month so that your IT Audit team can verify that their access processes are working successfully.

From: Lacroix, Fiona
Sent: October 25, 2016 11:16 AM
To: Brollosy, Mike
Subject: Information Requested

Hi, Mike –

I am happy to provide the information that you requested. The table below includes our records of the access level of the last ten people who joined StellanTECH.

<table>
<thead>
<tr>
<th>Employee name</th>
<th>Permissions requested</th>
<th>Start date</th>
<th>Access approval date</th>
<th>Access date</th>
<th>Permissions granted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emily Madison</td>
<td>End-User</td>
<td>10/3/2016</td>
<td>10/6/2016</td>
<td>10/10/2016</td>
<td>End-User</td>
</tr>
<tr>
<td>Ethan Monroe</td>
<td>End-User</td>
<td>10/17/2016</td>
<td>10/14/2016</td>
<td>10/17/2016</td>
<td>End-User</td>
</tr>
<tr>
<td>Leslie Nguyen</td>
<td>End-User</td>
<td>10/10/2016</td>
<td>10/7/2016</td>
<td>10/10/2016</td>
<td>End-User</td>
</tr>
<tr>
<td>Olivia Johnson</td>
<td>End-User</td>
<td>10/10/2016</td>
<td>10/6/2016</td>
<td>10/10/2016</td>
<td>End-User</td>
</tr>
<tr>
<td>Jacob Kim</td>
<td>End-User</td>
<td>10/10/2016</td>
<td>None</td>
<td>10/10/2016</td>
<td>Systems Administrator</td>
</tr>
<tr>
<td>John Smith</td>
<td>End-User</td>
<td>09/26/2016</td>
<td>9/22/2016</td>
<td>9/26/2016</td>
<td>End-User</td>
</tr>
<tr>
<td>Laurie Liu</td>
<td>End-User</td>
<td>10/10/2016</td>
<td>10/14/2016</td>
<td>10/17/2016</td>
<td>End-User Power User</td>
</tr>
<tr>
<td>Madison Jenkins</td>
<td>Power User</td>
<td>10/10/2016</td>
<td>10/13/2016</td>
<td>10/17/2016</td>
<td>Power User</td>
</tr>
<tr>
<td>Sam Washington</td>
<td>End-User</td>
<td>10/17/2016</td>
<td>10/17/2016</td>
<td>10/17/2016</td>
<td>End-User</td>
</tr>
</tbody>
</table>

Table 2: Access levels of people

The table below includes a sample of 10 people who left the company within the last month.

<table>
<thead>
<tr>
<th>Employee</th>
<th>Termination</th>
<th>Termination reason</th>
<th>Deactivation date</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Date Start</th>
<th>Date Exit</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daniel Kim</td>
<td>9/26/2016</td>
<td></td>
<td>Retired</td>
</tr>
<tr>
<td>Carlos Rodriguez</td>
<td>10/10/2016</td>
<td>10/17/2016</td>
<td>Resigned</td>
</tr>
<tr>
<td>Jill Jones</td>
<td>10/17/2016</td>
<td></td>
<td>Fired</td>
</tr>
<tr>
<td>Rachel Tanaka</td>
<td>10/3/2016</td>
<td>10/10/2016</td>
<td>Resigned</td>
</tr>
<tr>
<td>Jim Douglas</td>
<td>10/3/2016</td>
<td>10/10/2016</td>
<td>Resigned</td>
</tr>
<tr>
<td>John Smith</td>
<td>10/10/2016</td>
<td>10/17/2016</td>
<td>Resigned</td>
</tr>
<tr>
<td>Richard Wang</td>
<td>10/10/2016</td>
<td>10/17/2016</td>
<td>Resigned</td>
</tr>
<tr>
<td>Jay Benton</td>
<td>10/3/2016</td>
<td></td>
<td>Fired</td>
</tr>
<tr>
<td>Sally Adams</td>
<td>10/10/2016</td>
<td></td>
<td>Resigned</td>
</tr>
<tr>
<td>Linda Melbourne</td>
<td>9/26/2016</td>
<td>10/3/2016</td>
<td>Resigned</td>
</tr>
</tbody>
</table>

Table 3: People who have left the company

Let me know if you need anything else or have any questions.

Best,
Fiona

Sent: Monday, October 24, 2016 10:51 AM
To: Lacroix, Fiona
From: Brollosy, Mike
Subject: Information Request

Hi, Fiona –

I hope you’re doing well. Thanks again for your help yesterday understanding the steps you take to grant and remove access to Critical. When you have time, please send me the following?

1. A list of ten new employees who started this month and level of permission they requested to Critical. Please include their start date, computer system approval date, computer system access date, and the actual level of permissions granted.
2. A list of the employees who exited the company, their termination date, termination reason, and their computer system deactivation date.

Thank you,

Mike Brollosy
KPMG

StellanTECH Critical System Audit Report Template- Exhibit 3

Title Page

Fiscal Year 2016 Report of the StefenTech Critical Information System

Prepared for Luca Stefen and Blair Alden

As of 1 March 2016

Prepared by Student Names

Executive Summary
Team 1 was contracted to perform an IT Audit for StellanTECH in order to provide process recommendations with a focus on StellanTECH’s most important computer system, Critical. The company is doing many things correctly. However, since this is the company’s first audit, it is understandable that more potential issues were identified as compared to a future audit.

Note: Students will add 2-3 paragraphs summarizing the information that they added in the remainder of the report. The Executive summary should be no more than a page in length.

**Background**

Our team was contracted to perform an IT Audit for StellanTECH in order to provide process recommendations with a focus on StellanTECH’s most important computer system, Critical. This is the company’s first IT Audit.

**Objectives and Scope**

**Objective:**

IT Auditors will provide process recommendations for the IT system called Critical. The Access Control Process, Process Flow, Configuration Management Process, and Contingency Planning Process will be reviewed as part of the audit.

**Scope**

Note: Students will provide a paragraph of information for each of the following sections.

- Access control process
- Process flow
- Configuration management process
- Contingency planning process

**Results**

Note: Students will provide conditions/weaknesses, possible effect, and a recommendation for each of the four sections listed above under Scope. The length of the results may vary from ½ - 1 page for each item.

**Conclusion**

The items listed above should receive the company’s attention in minimize the risk. All of the items identified have recommendations that will help the company in doing so.
Access Controls Documentation Report - Exhibit 4

The tables below list sample examples for the instructor of the various conditions that the students should identify in the case and includes the conditions/weaknesses, possible effect, and a recommendation for each.

<table>
<thead>
<tr>
<th>Conditions/Weaknesses</th>
<th>Possible Effect</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>When hiring a new employee, no background check is performed.</td>
<td>The company’s likelihood of hiring someone who may compromise the corporate assets is increased.</td>
<td>When hiring a new employee, perform a background check.</td>
</tr>
<tr>
<td>In some cases, no record of when the access was granted to someone is recorded in the database</td>
<td>The company cannot easily identify who has access to what and if their level of access is correct.</td>
<td>This information should be retained.</td>
</tr>
</tbody>
</table>

Table 4: Access control process conditions/weaknesses, possible effect, and recommendations

Process flow

<table>
<thead>
<tr>
<th>Conditions/Weaknesses</th>
<th>Possible Effect</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>When a new customer is created, the system automatically scans the other customer names looking for duplicates. If no duplicates are found, the account is marked “new.”</td>
<td>Existing Customers may be categorized as new customers which could lead to extra dollars being spent on bonuses.</td>
<td>This process is insufficient to determine whether a customer is new or not. Additional validation should occur.</td>
</tr>
</tbody>
</table>

Table 5: Process flow conditions/weaknesses, possible effect, and recommendations

Configuration Management Process

<table>
<thead>
<tr>
<th>Conditions/Weaknesses</th>
<th>Possible Effect</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Quality Assurance (QA) team allocates their time testing updates based on which updates are determined to be significant.</td>
<td>Some system updates may be implemented that have not been fully tested.</td>
<td>All system enhancements and updates should be tested.</td>
</tr>
<tr>
<td>The CCB review and approval process is sometimes skipped if the project is running behind schedule.</td>
<td>Some system updates may be implemented that have not been fully tested or approved.</td>
<td>This process should not be skipped.</td>
</tr>
</tbody>
</table>

Table 6: Configuration Management Process conditions/weaknesses, possible effect, and recommendations
Contingency Planning Process

<table>
<thead>
<tr>
<th>Conditions/Weaknesses</th>
<th>Possible Effect</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data in the Critical system is replicated every Wednesday from the primary processing site in Washington, DC to an alternate processing site in Omaha, Nebraska on a near real-time basis</td>
<td>If a data restoral is necessary, not all of the data is current.</td>
<td>The system updates should be occurring on all days.</td>
</tr>
</tbody>
</table>

Table 7: Contingency planning process conditions/weaknesses, possible effect, and recommendations

Case Conclusion

IT Auditing can be difficult for students to understand in an introductory MIS or CIS course. This case can help to bridge that gap in a relevant way.